Did You Read Your STIG Today?

December 2010

Cleaning up after a real mess is no fun. Anyone with kids, pets, a party-hearty roommate, or in-laws that stay for more than a few days knows this is true. The process usually involves rubber gloves, face masks and clothing that you are prepared to burn when you're finished. Cleaning a computer, or a network, after it has been infected can be just as bad. Your hands may not smell as funny when you're done, but there's that nagging sleep-depriving feeling that maybe you didn't get it completely clean. You may have no choice when it comes to the kids and in-laws, but network contamination is a mess you can avoid.

There are two aspects to cyber security, the technical – firewalls, anti-virus, software, ad blockers – and the human. The human aspect carries the most risk, because it often relies on a number of people to follow safe cyber procedures and exercise some common sense consistently and uniformly. Right now you are thinking, "Joe and Susan never do what they are supposed to do." They may be thinking the same thing about you. Even if people try to practice sound information assurance, it is often difficult to keep up with some of the policies and procedures because technology moves at such a fast pace. This is true not only in military, government and private sector settings, but also in our own homes. Often network intrusions are not due to malicious or negligent actions, but to lack of understanding of what needs to be done. That's where Security Technical Implementation Guides (STIGs) come in.

STIGs are information assurance and cyber security guidelines. They are developed by The Defense Information Systems Agency (DISA) Field Security Operations (FSO) Standards and Guidance Branch and provide detailed configuration information about software and hardware that minimizes network-based attacks and secures information against malicious threats.

STIGs can help protect information systems by providing ways to make them more secure. They cover a wide array of topics. Many of them are common to the home computer user as well with such topics as Instant Messaging, Antivirus Security Guidance and Browser Security Guidance. These are the step by step instructions that everyone can take advantage of to protect networks, systems and computers. Many of the practices described can be applied at home as well as in the office or in theater. So they can not only keep military data and operations safe, but your family's identity and online life as well.

These STIGs are readily available and can be accessed by anyone. Because they are broken down by category, you don't have to search through huge documentation binders or massive online files to find the part that covers what you need. By following the procedures and guidelines in them you can greatly reduce the human factor risk in cyber security. Ignorance is no longer a valid excuse for exposing a computer or network to worms and viruses. Using these guides carefully and consistently will definitely improve the cyber security of anyone who logs into a network, whether it's in Kabul or here at home. So, let Joe and Susan know about STIGs. More important, take advantage of them yourself. After all, the best kind of leadership is leadership by example.

More information on STIGs, plus a mailing list signup is available at the Information Assurance Support Environment (IASE) Home Page, sponsored by The Defense Information Systems Agency (DISA): http://iase.disa.mil/stigs/index.html.

Have a Happy and virus and intrusion-free holiday season from SFC Firewall and the On Cyber Patrol Team. Also, because a secure cyber home front is as important as a secure perimeter in a war zone, watch for "The Family Firewall," coming in January. Seems the Sarge has a family that needs information assurance and cyber security guidance as well.